Exhibit D

Scalable Intrusion Detection for the Emerging Network Infrastructure

Objective

What: This three-year DARPA-funded project is to design and develop a software system for protecting against intruders from breaking into network routers, switches, and network management channels. The project is a joint collaboration between MCNC and North Carolina State University (NCSU).

Why: Given the increasing popularity of the Internet, intrusion incidents are becoming common events of life. Attacks on the network infrastructure has the potential of disrupting a large scale of information services on which the national defense and economy may depend. Despite the best efforts of the protocol designers, implementors, and system administrators, it is prudent to assume that attacks will occur and some, unfortunately, will succeed. Therefore, it is vitally important to develop means to automatically detect and respond to these attacks in order to maintain these critical information services.

Approach

In this project, we will design, implement, and integrate intrusion detection techniques based on statistical and logical analysis of network routing and management protocols to construct a scalable distributed intrusion detection system for the emerging internetwork environment. At the top level, the system consists of local detection subsystems and remote management application subsystems. The integration of these two subsystems will be mapped onto the SNMP standard management framework.

A local subsystem has three major components: rule-based prevention module, protocol-based detection module, and statistical analysis detection module. As a gate-keeper, the prevention module intercepts and filters all incoming packets according to a small set of rules. It conducts a quick check to see whether an incoming packet violate general security guidelines or special administrative security concerns. A second component of the system uses logical analysis of protocol operation. This technique detects intrusion by monitoring the execution of protocols in a router/switch and triggering an intrusion alarms when an anomalous state is entered. The statistical-based approach is founded on the contention that network routing and management protocols exhibit certain behavioral signatures. Any behavior deviating from the normal signature will be considered as an anomaly and appropriate alarms can be triggered.

The detection functions of a local subsystem are complementary in nature in terms of their capabilities and their response times. The rule and protocol based approach is meant to analyze and detect known vulnerabilities. On the other hand, the statistical analysis is intended to uncover those attacks that cannot be prevented by a set of rules embedded in a rule-based component or cannot be detected by security analysis conducted through protocol-based approach. As far as response time is concerned, the statistical approach requires an observation window to determine whether the target is anomalous. The protocol-based and, especially, the rule-based mechanisms will be able to detect the targeted intrusions with relatively low latency.

For demonstration purposes, we will implement simple network management applications for accessing and coordinating local detection information. The choice of using SNMP as the information exchange protocol was based on the fact that it is standardized and any other security applications based on SNMP may potentially interoperate with our system with relative ease.

To evaluate the system design and implementation, we will develop a set of attacks and use them to exercise our system by attacking nodes within a testbed network. These tests will allow us to measure the run-time overhead introduced by the intrusion detection system. After the validation process, we expect to deploy and evaluate the system in an operational network.

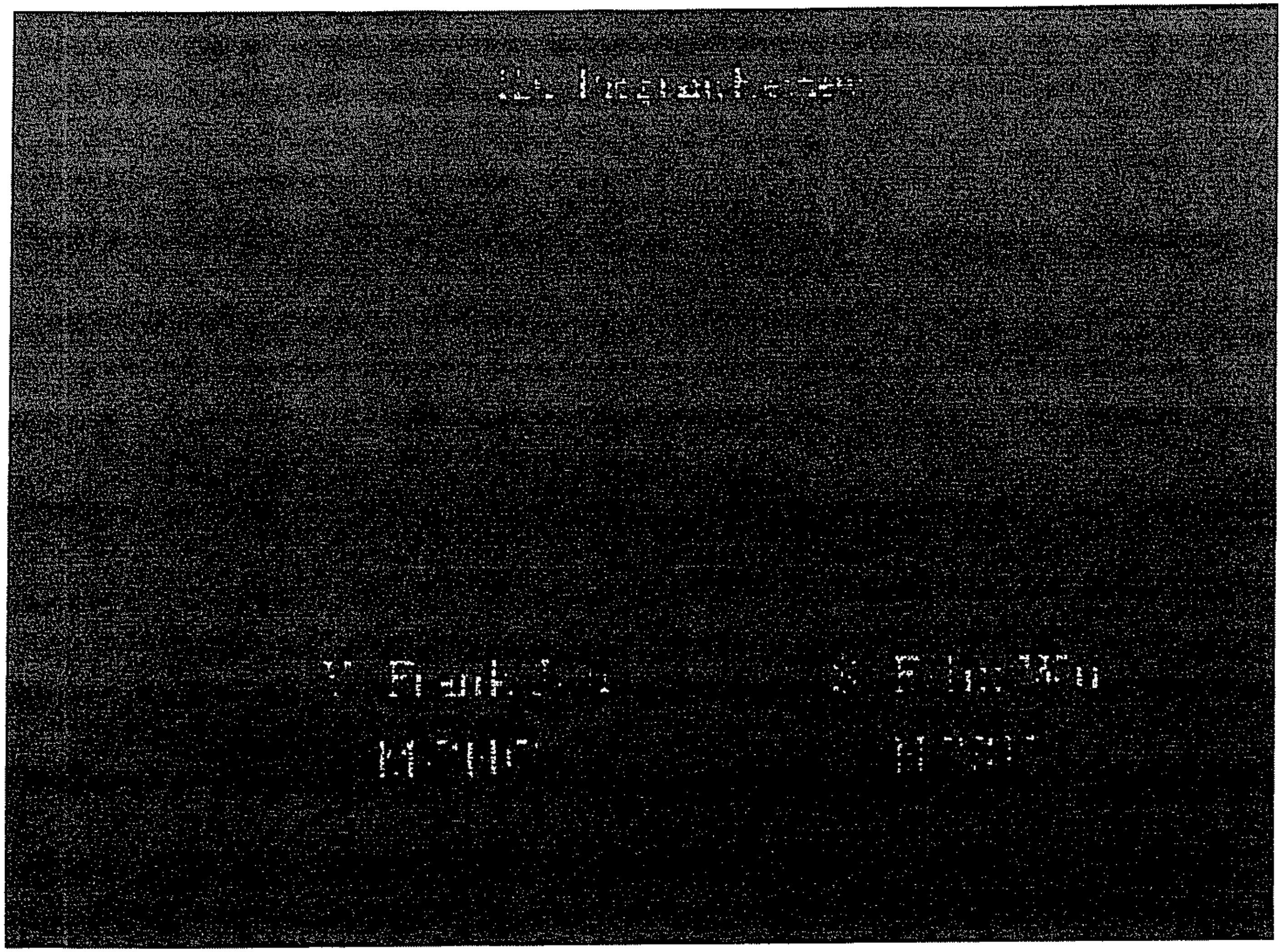
Related Information

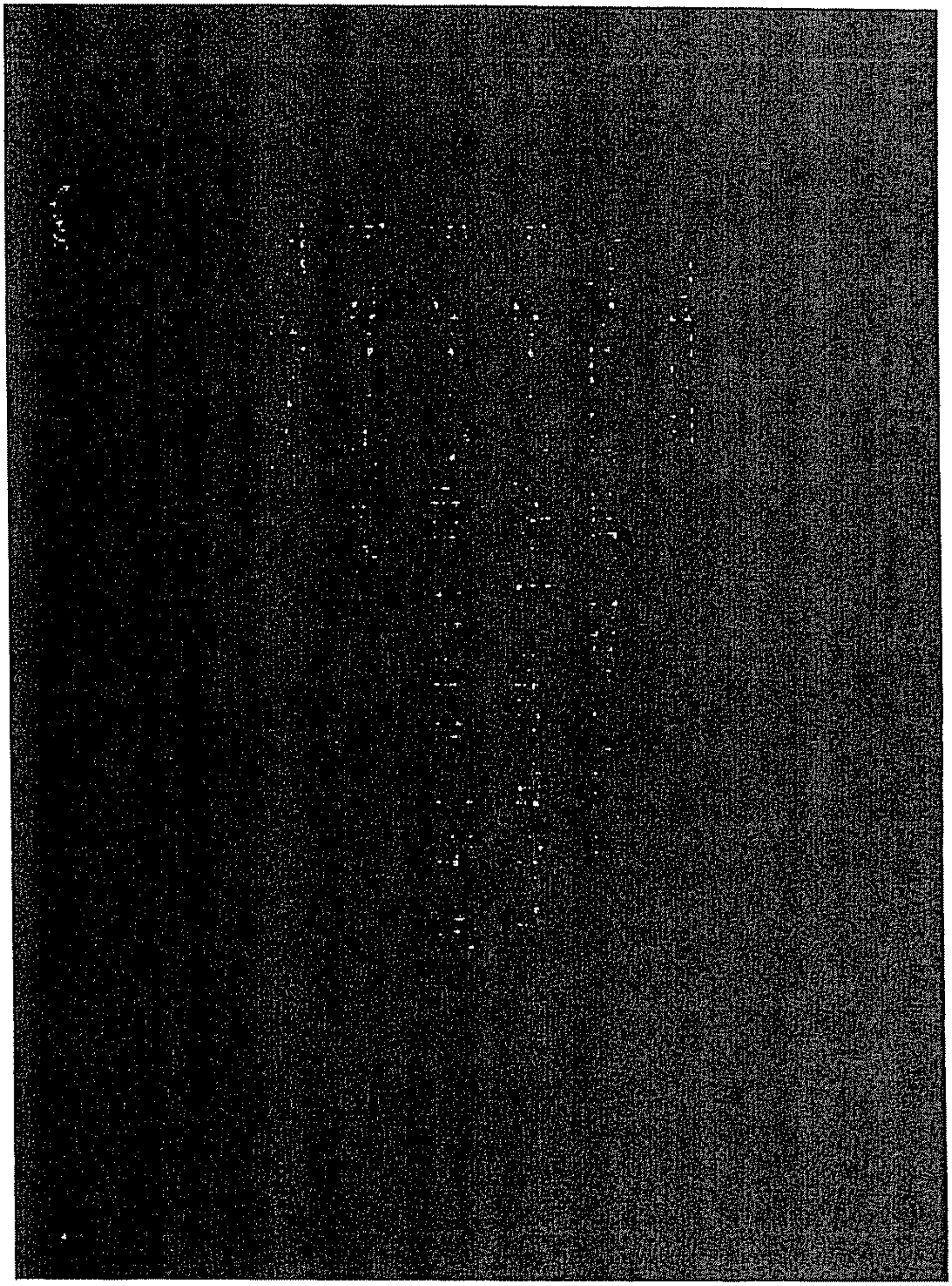
- Project Viewgraph (powerpoint)
- Architecture Design Report (postscript)
- Project Update Viewgraph (at SRI, July 97, powerpoint)
- Project Update Viewgraph (at Annapolis, MD, Feb. 98, powerpoint)

- Contact: Y. Frank Jou, Email: jou@mcnc.org

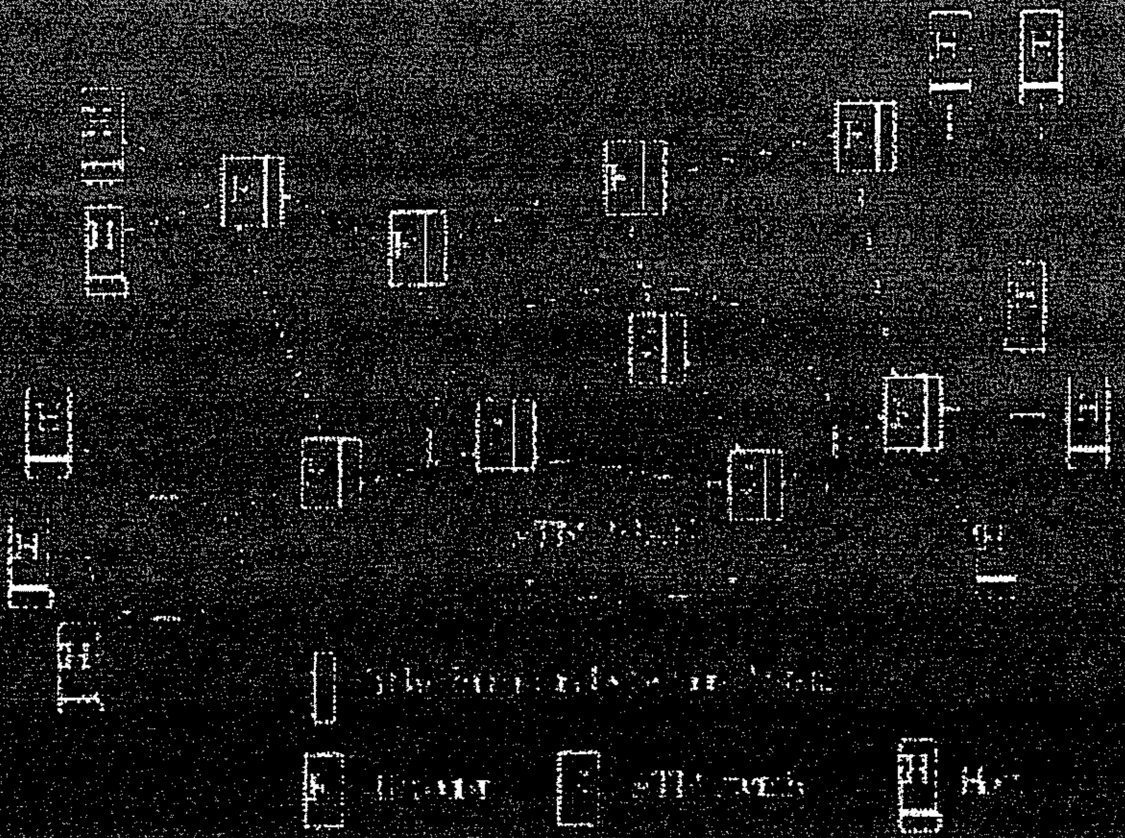
MCNC
Post Office Box 12889
Research Triangle Park
North Carolina 27709-2889

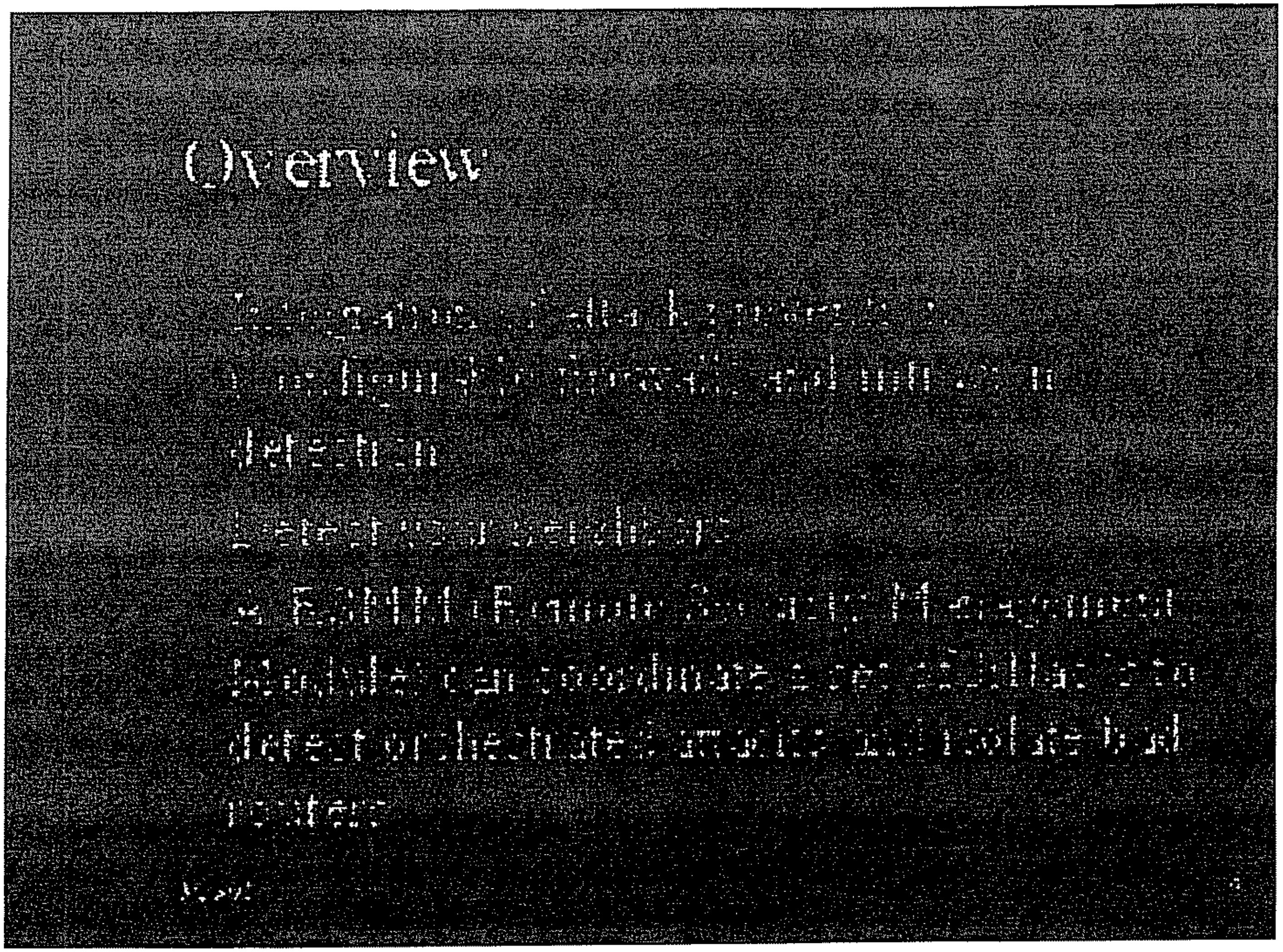
Last Modified: September 24, 1997





Overview





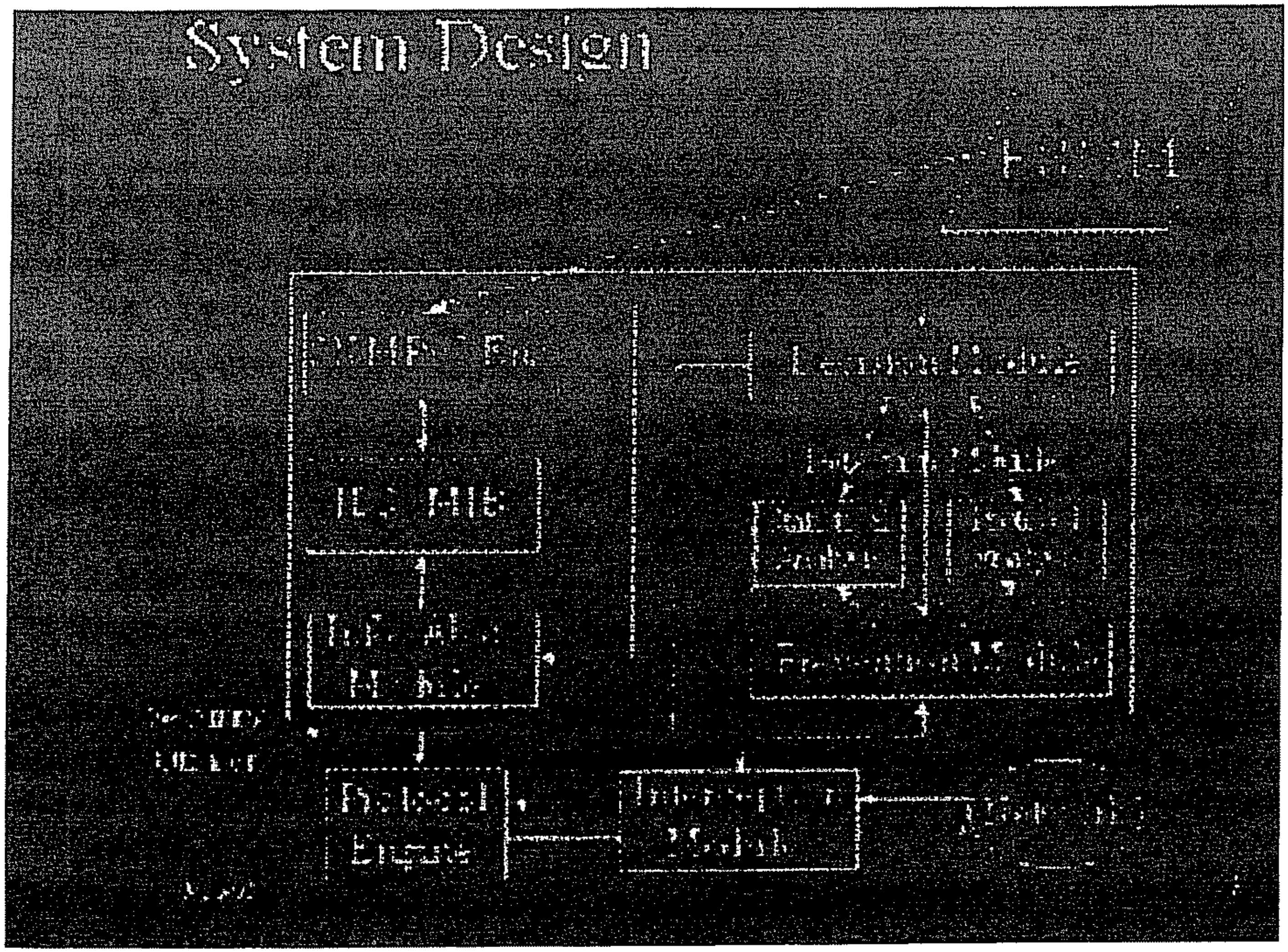
Overview

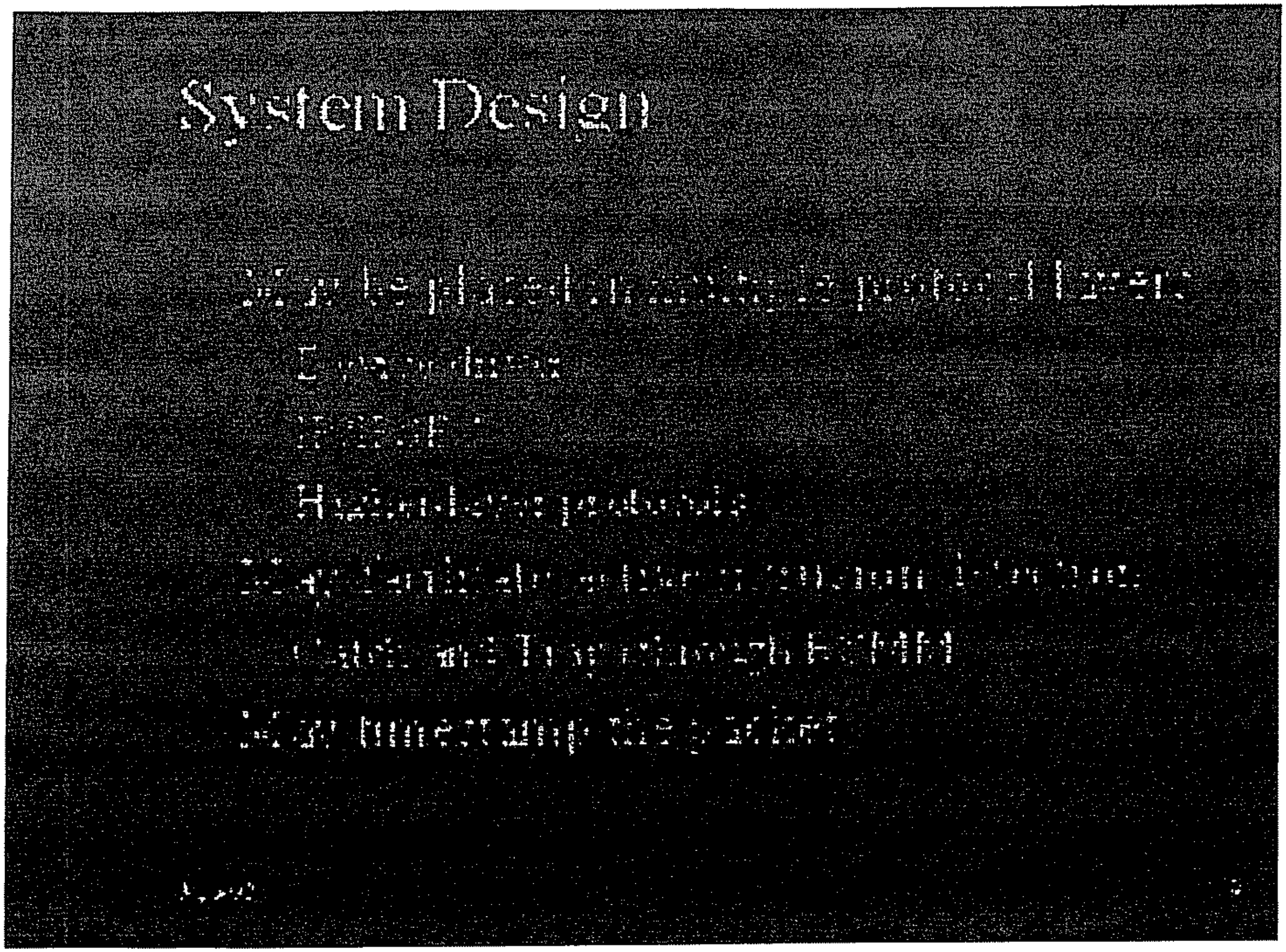
Integration of attack prevention technologies (firewalls and intrusion detection)

Detect router attacks

A RSMM (Remote Security Management Module) can coordinate a set of [illegible] to detect orchestrated attacks and isolate bad routers

System Design





System Design

- May be placed at multiple protocol layers
  - Device drivers
  - IPSEC
  - Higher-level protocols
- May facilitate collaborative intrusion detection
  - Catch and Trap through SNMP
- Must timestamp the packet

System Design

- Presentation Layer [illegible]
  - [illegible]
- [illegible] Layer
  - HTML [illegible]
  - [illegible]
    - [illegible]
      [illegible]